

Connectez-moi!

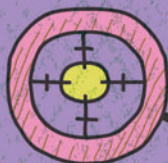


*Martin Untersinger*

Préface de Benjamin Bayart

# ANONYMAT *sur* INTERNET

Comprendre pour  
protéger sa vie  
privée



EYROLLES

# Préface

C'est devenu une banalité, fausse, que de dire qu'Internet est en train de changer nos sociétés. Sauf à lui supposer une origine divine, Internet n'a pas été imposé à la société depuis l'extérieur ni n'est en train de la réformer contre son gré. Internet est l'outil dont les sociétés humaines occidentales se sont dotées pour évoluer, pour changer. Ce changement prend bien des formes, et touche bien des aspects, dont les mieux compris et analysés touchent à l'échange de biens immatériels et à la liberté d'expression.

Concernant l'échange des biens immatériels, par exemple le partage de fichiers musicaux ou de vidéo, la caricature du vol souvent employée n'a pas de sens, puisque l'ancien exemplaire du fichier est *toujours* sur le disque dur où il se trouvait auparavant. Si le fait de regarder la baguette de pain dans la vitrine en fait apparaître, magiquement, une nouvelle dans ma main, je ne vole pas le boulanger. Cet échange de biens immatériels a des conséquences sur les modèles économiques de nombreuses industries, à commencer par celle du divertissement. Quand on fait métier de vendre des copies sur support plastique, comment survivre à l'apparition de la fantastique machine à copier qu'est Internet ?

Quant à la liberté d'expression, c'est simplement le fait que chaque citoyen puisse s'exprimer publiquement, et ait l'opportunité d'être lu et entendu par tous. Au siècle dernier, protéger la liberté d'expression, c'était protéger la liberté de la presse. La seule forme d'expression accessible au commun était alors la discussion autour de la table au dîner de Noël, ou au café du coin. Ce qui était, au siècle dernier, réservé à une minorité (journa-

listes, artistes, dirigeants divers, etc.) est maintenant accessible à tous. Quiconque a un mur Facebook, un blog, un compte Twitter, un tumblr, dispose d'un lieu d'expression qu'il peut ouvrir au public. Sur Internet, tout le monde est éditeur de ce qu'il publie, tout le monde est éditorialiste et chroniqueur. La question des libertés, et des règles de société, qui vont avec cette expression publique, est une question majeure de l'organisation des sociétés post-Internet, une question politique : comment voulons-nous faire société ensemble ?

Cette question se décline en de nombreuses facettes. À commencer par celle du pouvoir qu'ont certains intermédiaires techniques sur notre vie numérique. Tout ce que je dis et fais sur Internet passe par mon fournisseur d'accès. Quel pouvoir de censure a-t-il ? Quel pouvoir d'intrusion a-t-il ?

C'est une des premières questions que je me suis posées sur le sujet, il y a plus de 15 ans. J'y ai répondu en ayant un accès Internet dans une association loi 1901, FDN, ce qui à l'époque était classique. J'y ai répondu en reprenant la présidence de l'association pour qu'elle ne disparaisse pas, pour que l'accès à Internet ne soit pas forcément une marchandise, et qu'il continue de pouvoir être autre chose qu'une marchandise. Et en étant toujours, en 2013, dix-sept ans plus tard, abonné d'un fournisseur d'accès associatif.

Les intermédiaires techniques sont nombreux à avoir un fort pouvoir de nuisance dans le monde numérique. Outre le fournisseur d'accès, il y a également le fournisseur de l'ordinateur (que ce dernier ait la forme d'un téléphone n'y change rien), ou le fournisseur de logiciel. Ces questions-là sont anciennes également. Pour ma part, j'ai fait le choix évident du logiciel libre précisément pour ces raisons : *mon* ordinateur fait ce que *je* veux, plutôt que ce qu'un éditeur a choisi qu'il fasse pour des raisons qui ne sont pas les miennes.

Les grandes plates-formes de services sont finalement d'apparition plus récente, au milieu des années 2000. Mais leur place

au cœur de l'expression publique de chacun devient centrale et donc dangereuse. Là aussi, la question qui revient est toujours la même : qui est capable de décider, qui peut censurer, qui rend des comptes ? Au final, est-ce moi qui suis libre de m'exprimer, ou est-ce Twitter qui tolère ce que je dis aussi longtemps que ça l'arrange ?

Enfin, il y a la question de l'identité, encore mal comprise. Pourtant, les personnes qui s'expriment publiquement ont toujours pu le faire sous une identité qu'ils ont choisie, sculptée, choisissant le nom, mais aussi la personnalité qu'ils montrent au public. Pour preuve l'exemple simple de Johnny Hallyday, dont tout le monde se fiche de savoir qu'il s'appelle J.-P. Smet. Et ce n'est pas un privilège d'artiste. On peut également se faire élire président de la République sous un pseudonyme, comme ce fut le cas de Nicolas Sarközy de Nagy-Bocsa, élu sous le nom de Nicolas Sarkozy, sans tréma ni particule. Même le président des États-Unis est connu dans le monde entier sous le nom de Bill Clinton, alors que son prénom est William. Jusqu'au Pape, qui règne sous un faux nom.

Lorsqu'on prend la parole en public, on choisit le nom sous lequel on apparaît. Cette identité-là n'est pas forcément celle de l'état-civil, mais c'en est bien une. Qui, d'ailleurs, ne connaît quelqu'un dont le prénom dans la vie courante diffère de ceux inscrits sur sa carte d'identité, ou n'est pas le premier de ceux-là, ou encore n'est pas orthographié de même ?

Les identités sous lesquelles on souhaite apparaître peuvent être multiples, et pour de multiples raisons. On peut par exemple ne pas avoir le même nom dans un réseau militant (Chaban) et dans le monde politique (Delmas). Le choix de l'identité sous laquelle chacun s'exprime, en fonction du lieu et du contexte, relève des libertés attenantes à la liberté d'expression. Et ce droit relève, forcément, du droit de s'exprimer sans donner de nom, du droit à l'anonymat.

La question des identités, à l'heure du numérique et donc de la surveillance généralisée, est une question politique clé, une question majeure sur la façon dont nous voulons faire société. J'en prend un exemple simple : l'Assemblée Générale qui m'a élu président du Fonds de Défense de la Neutralité du Net l'a fait sans voir mes papiers d'identité. C'est l'individu qui s'exprime dans l'espace public sous le nom de Benjamin Bayart, reconnaissable à sa barbe et à ses cravates ridicules, qui a été élu à ce poste. Pourtant, c'est à la carte d'identité que le banquier a accordé la signature sur un compte bancaire. D'une certaine façon, le banquier n'a pas respecté le vote de l'Assemblée Générale, pourtant souveraine sur la question. Il a supposé que le Benjamin Bayart de l'état-civil était le même que celui de l'espace public.

Une forme numérique assez simple est pourtant au point depuis vingt ans : ma clef de chiffrement publique, qui est... publique. L'Assemblée Générale aurait pu élire comme président « la personne qui s'exprime avec cette signature », et le banquier aurait pu contrôler cette information, bien plus fiable que ce que raconte le support de plastique distribué par l'État. Ainsi il m'appartient de savoir et de faire savoir qui je suis, il m'appartient de me nommer, et l'état-civil ne sert qu'à enregistrer celui de mes noms qui servira dans mes échanges avec l'administration, ou lors du prochain recensement.

Les questions autour des identités, autour de l'anonymat qui en est le corollaire immédiat, autour du droit de ne pas être surveillé, autour du droit à la vie privée, sont des questions majeures pour comprendre la société qui est en train de se construire avec Internet. Et c'est une des questions qui restent le plus mal connues, même des spécialistes.

Benjamin Bayart

Président de la fédération FDN

(Fournisseurs d'accès à Internet associatifs)

# Table des matières

## 1. Anonymat sur Internet : de quoi parle-t-on ? 1

Bien définir l'anonymat 1

Un anonymat tout relatif 2

Sur Internet, l'anonymat ne cache qu'une partie de son identité 2

Neutralité (morale) de l'anonymat 3

Définition de la vie privée 3

La vie privée, une nécessité selon Montaigne 3

La vie privée numérique, c'est le contrôle 5

Problème : on n'a pas toujours le contrôle 5

Pourquoi Internet chamboule tout 6

Un renversement : une vie publique par défaut,  
privée seulement parfois 7

Internet berceau de la vie publique 7

Traces involontaires et invisibles 8

Le pseudonymat 9

## 2. Sur Internet, l'anonymat n'existe pas 11

Une pression croissante de l'État 11

Pour contrôler, il faut savoir qui est qui et qui fait quoi 12

Un exemple français : la conservation des données de connexion 13

Comment ça marche ? 14

L'anonymat remis en question par des intérêts économiques 15

Valeur des données personnelles

pour les « e-commerçants » 17

Un modèle économique reposant sur votre identité... 18

... donc hostile à l'anonymat et au pseudonymat 19

L'anonymat, un obstacle au modèle économique du Web 19

Un dilemme insurmontable : communiquer ou laisser des traces ? 21

La menace des « trackers » publicitaires 21

Comment les entreprises font-elles pour vous surveiller ? 22

Où se cachent les mouchards ? 23

Les données collectées par les trackers sont anonymisées :  
un mythe ? 24

Les données ne sont jamais anonymes 25

Des critiques de films peuvent révéler une identité 25

Identification par des requêtes dans un moteur de recherche 26

Le dossier médical d'un gouverneur identifié 27

Les informations publiées sur le Web nous font-elles  
courir à notre ruine ? 28

### **3. De l'intérêt de l'anonymat 31**

L'anonymat, une histoire de contrôle 32

Être qui on veut 32

Le pseudonymat 33

L'anonymat et la liberté 34

L'anonymat, nécessaire à la liberté d'expression ? 34

L'anonymat protégé par la justice 35

L'argument « Je n'ai rien à cacher » 36

Un argument un peu absurde 36

Trois exemples pour le réfuter 37

L'anonymat et le droit 39

Qu'est-ce que la vie privée ? 40

Des dispositions plus précises dans d'autres textes juridiques 41

Vers un véritable droit à l'anonymat ? 42

Le droit est parfois mal adapté 42

Typologie des menaces 43

Les entreprises 43

L'État et la police 45

Piratage et défaillances 46

Vos proches 47

## 4. Les bases de la protection 49

- Identifier ses ennemis et estimer le risque 49
  - Les six menaces pour votre vie privée 50
  - Différencier risque et menace 51
  - Les cinq commandements de l'anonymat 52
- Être anonyme : se protéger d'une menace inconnue 54
  - L'anonymat dépend des autres 54
  - Un échange, plusieurs vulnérabilités 55
  - Les questions à se poser 56
- Le navigateur 58
  - Naviguer, c'est quoi ? 58
  - Quel navigateur choisir ? 60
  - Pourquoi importe-t-il de protéger son navigateur ? 61
  - Ne pas laisser de traces avec son navigateur 63
  - Désactiver ou supprimer l'historique de navigation 65
  - En résumé 65
  - Mode navigation privée 66
  - Cookies 67
    - « HTTPS everywhere » 69
  - Les requêtes HTTP 71
  - L'adresse IP 72
  - D'autres outils plus complexes pour dissimuler les traces du navigateur 73

## 5. Géants et entreprises du Web 75

- Comment savoir quelles traces j'ai laissées ? 76
  - Traces volontaires 77
  - Traces involontaires 77
- Évaluer les risques en souscrivant à un service 78
  - Conditions générales d'utilisation, « terms of service » et politiques de vie privée 78
  - Les questions à se poser avant d'utiliser un service 80
- Protéger son identité chez les géants du Web 81



Le cas Google 82

Disparaître du Web (et récupérer ses données) 85

Faire une dernière sauvegarde 86

Peut-on faire confiance à un géant du Web ? 87

Déjouer le pistage à notre insu 89

Empêcher les réseaux sociaux de nous suivre 89

Empêcher les publicitaires de nous suivre 91

Quelques principes avant de télécharger une extension  
ou un programme 95

## **6. Communiquer : e-mails et discussions instantanées 97**

Qu'est-ce qu'un e-mail ? Comment circule-t-il ? 97

Un peu de vocabulaire 98

Différence entre les protocoles de courriel POP et IMAP 98

Les vulnérabilités de l'e-mail 99

Comment choisir votre fournisseur de mail ? 101

Les webmails commerciaux 101

Solutions d'e-mail alternatives 103

Se protéger 105

Adresse e-mail jetable :

vers un e-mail propre 107

Cryptographie et chiffrement 109

Qu'est-ce que la cryptographie ? 109

Comment la cryptographie protège-t-elle les messages ? 109

Vocabulaire de la cryptographie 110

De quoi est constitué OpenPGP ? 111

Le système de clef privée et de clef publique 112

Générer sa clef 113

Empreinte et signature 114

Signer ses messages 115

Chiffrer ses e-mails avec Enigmail 116

Créer sa clef 117

- Envoyer la clef sur le serveur 119
- Stocker ses clefs 120
- Envoyer un message chiffré et signé 120
- Les problèmes posés par OpenPGP 121
- Le chiffrement ne suffit pas 123
- Si vos contacts n'utilisent pas OpenPGP :  
utilisez une boîte aux lettres morte 124

#### Message instantanée 125

- Chiffrer vos discussions instantanées avec OTR 128

#### Discuter en son et en images : la voix sur IP (VOIP) 131

#### L'erreur humaine 133

## **7. Protéger sa connexion : proxies, VPN et le projet Tor 135**

### Les proxies 135

- Les proxies, comment ça marche ? 136
- Limitations du proxy 136
- Les proxies web, HTTP et SOCKS 138
- Comment utiliser un proxy ? 139
- Logiciels et extensions pour gérer les proxies 141

### Les réseaux privés virtuels ou VPN 142

- Qu'est-ce qu'un VPN et comment marche-t-il ? 142
- Points négatifs à l'utilisation d'un VPN 143
- Comment configure-t-on son VPN ? 145
- Comment choisir son VPN ? 147

### Tor, la solution la plus aboutie 151

- Comment Tor fonctionne-t-il ? 152
- Comment utiliser Tor ? 153
- Tor est-il vraiment sécurisé ? 156
- Autres réseaux anonymes 156

## **8. Se protéger mieux et aller plus loin 159**

### Protéger son mobile 159

- Les faiblesses de votre téléphone 160

Utiliser un VPN avec son téléphone 162

Solutions tout-en-un : tout faire avec un seul outil 162

Sécuriser ses messages texte 163

Chiffrer ses appels 163

Naviguer de manière sécurisée 163

Gérer les autorisations des applications 164

Protéger son mot de passe 164

Vulnérabilité inhérente 165

Les commandements du bon mot de passe 165

Des logiciels pour stocker vos mots de passe 168

Systèmes d'exploitation orientés sécurité 168

Les fournisseurs d'accès à Internet (FAI) 169

Aider ceux qui veulent être anonymes 170

Aider les utilisateurs de Tor 171

Donner de la bande passante... ou de l'argent ! 172

S'informer et aller plus loin 173

## **9. Entre la chaise et le clavier 177**

Ne jamais faire confiance 178

Comparer les coûts et les risques, et s'adapter en fonction 178

Internet n'est pas fait pour l'anonymat 180

Comment choisir ses armes ? 182

Choisir des outils utilisés par une large communauté  
d'utilisateurs 182

Utiliser des logiciels libres 184

Sélectionner une infrastructure décentralisée 186

Méfiez-vous des entreprises 186

Identifier votre « ennemi » 188

L'erreur humaine et l'entraînement 189

## **10. Quel avenir pour l'anonymat ? 191**

Des réformes s'annoncent 192

Des pistes non étatiques 193

La solution par les entreprises ? 194

Vous avez dit démocratie ? 195

Les effets néfastes de l'anonymat ? 197

Le double jeu des politiques 198

Renversement de paradigme 199

**Notes de fin 201**

**Bibliographie 209**

**Index 213**

# Avant-propos

*L'anonymat sur Internet souffre d'un paradoxe étrange. Alors qu'on utilise de plus en plus Internet, qu'on y laisse toujours plus de données et qu'il est de plus en plus facile de savoir qui y fait quoi, l'inquiétude quant à l'utilisation de ces données grandit chaque jour.*

## Pourquoi ce livre ?

Jamais anonymat et vie privée n'ont été à ce point discutés et débattus. Et pour cause, sur l'Internet d'aujourd'hui, l'asymétrie d'information est totale : si on voit bien les usages qu'on peut tirer de services gratuits « offerts » par Google et Facebook (ou autres sites financés par la publicité), ces derniers savent très bien que nos informations personnelles sont à la source de leur « création » de richesse.

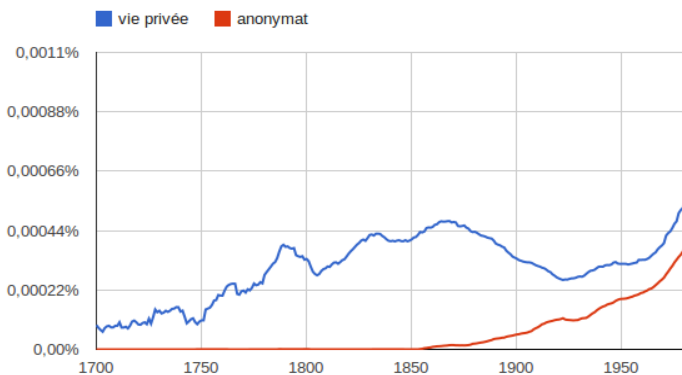


Fig. 0-1 > L'évolution des termes « vie privée » et « anonymat » dans le corpus de livres indexés par Google

L'internaute non averti, lui, ne sait absolument pas quel type d'information personnelle il donne, quand il la donne, pour combien de temps, dans quel but ou pour quel profit, ni même, parfois, qui la collecte.

#### CHIFFRES L'humanité, ou presque, sur Internet

À l'heure où nous écrivons ces lignes, il y a un demi-milliard d'utilisateurs sur Twitter<sup>1</sup>, un milliard sur Facebook<sup>2</sup> et près de 200 millions de blogs<sup>3</sup> ; on n'a jamais autant parlé de soi sur Internet. Pour autant, la vie privée et l'anonymat n'ont jamais été aussi importants pour les internautes, à rebours d'un discours ambiant banalisant le naturisme numérique.

Sur un réseau dont la mémoire et les capacités de copie sont en théorie illimitées, nul ne sait ce que nous prépare l'accumulation de données, traces et autres informations personnelles que nous laissons par téraoctets entiers, quotidiennement, sur Internet.

EN SAVOIR PLUS **L'hypermnésie**

Vous pouvez consulter à ce sujet la section consacrée à l'hypermnésie, du manuel *Informatique et sciences du numérique*.

 *Informatique et sciences du numérique*, Gilles Dowek *et al.*, Eyrolles, 2012.

Une véritable option d'informatique a enfin fait son entrée au lycée, à quoi répond ce manuel adressé aux lycéens de Terminale S ayant choisi la spécialité ISN. C'est un manuel que chacun peut (et devrait) lire – en tout cas tout lecteur souhaitant comprendre les bases de l'informatique.

C'est sans compter les utilisateurs situés dans des pays intolérants, prompts à la censure ou à l'intimidation, et les citoyens occidentaux, parfois effrayés par les velléités étatiques de contrôle et d'identification sur les réseaux et par les divers systèmes de traçabilité installés par les entreprises ou les particuliers.

Internet a beau être un média pensé et fait pour mener une vie publique, le glissement sur les réseaux de nos existences, de nos secrets et de notre intimité fournit de multiples raisons de protéger son anonymat et, de fait, son identité et sa vie privée.

Ce livre va tenter de vous donner une palette d'outils, de l'astuce la plus simple à la stratégie la plus complexe, pour comprendre et protéger les informations que vous laissez filer à chacune de vos connexions.

DÉFINITIONS **Anonymat, vie privée, identité, sécurité...**

Des thèmes connexes à l'anonymat seront évoqués et traités dans ce qui va suivre : vie privée, sécurité informatique... Il était difficile de faire autrement, tant ces domaines sont liés. Nous espérons, avec ce livre, faire un pont entre la théorie et la pratique, comprendre les mouvements en marche sur Internet pour mieux y adapter sa stratégie, comprendre le pourquoi pour appliquer le comment.

Sur Internet, « on ne peut pas ne pas laisser de traces<sup>4</sup>. » Pourtant, ces outils sont nécessaires à ceux que cette bataille interpelle, intéresse ou inquiète. Entre les grandes entreprises américaines qui tentent par tous les moyens de faire changer la perception de ce qui peut être privé et public sur le réseau, la peur bleue des gouvernements de ce qui se passe sur Internet et les initiatives individuelles ou émanant d'entreprises qui se vantent de toujours davantage protéger la vie privée des internautes, les lignes de démarcation sont floues et mouvantes. Nous espérons modestement vous donner quelques points de repères au fil de ces pages.

Quant aux protections et aux outils que nous aborderons, ils sont parfois difficiles à comprendre et à appliquer : les menaces sur votre identité sont multiples, et chacune présente ses caractéristiques propres. La sécurité est une question compliquée que l'on ne peut résoudre qu'en s'armant de temps, de patience et d'envie. Même si l'anonymat absolu n'existe pas, cela ne veut pas dire qu'il faut abandonner toute volonté de protection.

L'habitude est l'ennemie de la sécurité. Appliquer bêtement des processus et utiliser des logiciels sans comprendre leur fonctionnement peut tout autant vous mettre en danger que vous protéger. La sécurité informatique est un ensemble cohérent où tout se tient. Les processus et les réflexes qui lui sont associés changent en permanence selon les évolutions technologiques, étatiques, juridiques ou commerciales. La sécurité n'est jamais acquise. C'est pourquoi ce livre ne donnera pas une liste exhaustive et définitive des moyens de protéger son anonymat et sa vie privée.

PÉREMPTION **La technique évolue (vite)**

Dans le champ de la sécurité informatique, rien n'est jamais vraiment acquis. Certaines des solutions abordées dans cet ouvrage peuvent être obsolètes au moment de votre lecture, même si nous avons fait tout notre possible pour aborder uniquement des solutions éprouvées.



## Plan de l'ouvrage

Après avoir défini un certain nombre de termes et rappelé quelques principes du fonctionnement d'Internet concernant l'anonymat (**chapitre 1**), on démontrera que l'anonymat total n'existe pas (**chapitre 2**). Pour autant, les raisons pour camoufler ses traces et son identité sont nombreuses (**chapitre 3**). Après avoir abordé les bases de la protection (**chapitre 4**), on se penchera sur les stratégies à mettre en place pour contourner la surveillance des entreprises et des géants du Web (**chapitre 5**). Puis on apprendra à protéger ses communications, notamment ses e-mails et ses discussions instantanées (**chapitre 6**), avant de se pencher sur la protection de sa connexion (**chapitre 7**) et d'aborder quelques outils plus techniques pour ceux qui désireraient aller plus loin (**chapitre 8**). Avant de dresser quelques pistes sur l'avenir de l'anonymat et de la vie privée sur Internet (**chapitre 10**), on abordera les réflexes fondamentaux à adopter sans même installer le moindre logiciel (**chapitre 9**).

## Remerciements

Cet ouvrage n'aurait jamais vu le jour sans le premier modem, arrivé dans la maison familiale à la fin des années 1990, et sans Muriel Shan Sei Fan et son e-mail de février 2012.

Je tiens également à remercier Chloé, qui aura supporté de m'entendre déblatérer des heures durant sur la vie privée et la cryptographie pendant des mois en faisant mine de s'y intéresser (et pour le reste aussi). Il me faut également remercier l'équipe de Rue89, et plus particulièrement mes rédacteurs en chef, dont la confiance et la liberté qu'ils m'ont accordées sont pour beaucoup dans la réalisation de cet ouvrage, ainsi que les fidèles acolytes que sont Pirhoo, Mayeu et Pierre Alonso, pour leur aide et leurs relectures précieuses. Merci aussi aux

tenanciers et piliers de bars de la mailing-list « AH » (ils se reconnaîtront) pour leur humour, leurs gifs animés et leurs sarcasmes, précieux alliés des derniers jours de rédaction. Les internautes qui ont gentiment répondu à mes questions sur les réseaux sociaux doivent aussi être remerciés ici, dont (j'en oublie) : @lactualaloupe, @\_swayb, @nkgl, @barzin, @bmaly-novytych, @zefede, @Zizounnette, @\_LilyRUsh, @johan-hufnagel ou encore @szadkowski\_m. Enfin, sans les innombrables internautes, activistes, hackers et autres passionnés plus ou moins anonymes, qui ont passé du temps et de l'énergie à alimenter les ressources indispensables que sont *free.korben.info*, le site de l'EFF, les diverses publications du collectif Tactical Tech, le Cryptoparty Handbook, cet ouvrage ne serait pas ce qu'il est. Merci à eux.

# Index

## A

ACTA 12  
actifs 50  
Adblock Plus 91  
adresse IP 72, 181  
adversaires 50  
AIM 126  
anonymat  
    cinq commandements 52  
    définition 1  
    neutralité 3  
    partiel 2  
    relatif 2  
Anonymous 187  
anti-tracking 94  
appel 163  
    chiffrer 163  
application 164  
assets 50

## B

backdoor 185  
Big Brother 21  
boîte aux lettres morte 124  
boyd, danah 5, 33, 88, 89  
Broadwell, Paula 188

## C

carte d'identité blanche électronique 193  
Chahid-Noura, Noël 45  
chaise-clavier (interface) 178

chat 125  
chiffrement 109, 123  
    asymétrique 111  
    symétrique 111  
Chrome 60, 62  
Chromium 61  
Circumventor 173  
CISPA 12  
clef  
    génération 117  
    serveur 119  
    stockage 120  
clef privée 112  
clef publique 112  
Code 18 178  
Code 45 178  
Code des postes et des communications électroniques 170  
Code pénal 41  
Cohen, Julie E. 35  
cohérence 51  
collecte de données 76  
Commotion (réseau) 199  
conditions générales d'utilisation 78  
confidentialité 50, 110  
Conseil constitutionnel 40  
consistency 51  
Constitution américaine 35  
contrôle 51  
Corée du Sud 34  
coûts 178

cryptographie 109  
 cryptopartie 173  
 CyanogenMod 162

**D**

DADVSI 11  
 Dashlane 168  
 de Marco, Estelle 34  
 Déclaration des droits de l'homme de 1789 40  
 Didn't Read 79  
 Dingledine, Roger 183  
 Discretio 163  
 disponibilité 51  
 DMCA 12  
 DNS 73  
 Do Not Track 64, 93, 192  
 Doctorow, Cory 194  
 donnée anonymisée 24, 25  
 données de connexion 13  
 Drake, Thomas 180  
 Droidwall 164  
 droit à l'anonymat 42

**E**

Echelon 15  
 e-commerçant 16, 17  
 Electronic Frontier Foundation 63, 69, 174, 187  
 e-mail 97
 

- anonyme 107
- client 98
- en-tête 100
- jetable 107
- serveur 98
- vulnérabilité 99

 empreinte 114  
 Enigmail 116  
 entraînement 189

entreprise
 

- surveillance 22

 erreur humaine 189  
 European Privacy and Human Rights 46

**F**

Facebook 19, 20, 34, 85, 89  
 FDN 170  
 Firefox 60, 62  
 fournisseur d'accès à Internet (FAI) 13, 169, 170
 

- Fédération FDN 170

 fournisseur de mail 101  
 Freenet 156  
 Frontline Defenders 174

**G**

génération
 

- clef 113

 Gmail 83, 102  
 GnuPG 111  
 Google 82, 86
 

- Dashboard 82

 Google+ 19, 32  
 Guardian Project 162

**H**

habeas corpus numérique 192  
 Hadopi 12  
 harcèlement 33  
 historique de navigation 65  
 HTTP 71  
 HTTPS everywhere 69  
 Hushmail 104  
 hypermnésie XI

**I**

ICQ 126

identification 26  
 identités 92  
 IMAP 98  
 information  
   asymétrie 44  
 infrastructure décentralisée 186  
 Instagram 86  
 intégrité 50, 110  
 IRC 126

**J**

Jabber 126  
 jailbreaker 162  
 JAP 157  
 Jarvis, Jeff 8  
 JavaScript 71

**K**

keylogger 133  
 Korben 174

**L**

LCEN 11  
 Lessig, Lawrence 12, 32, 35, 194  
 Lewman, Andrew 32  
 Liberation Tech 174  
 liberté d'expression 34  
 little brothers 21  
 local 68  
 logiciel libre 184  
 logs 13  
 loi informatique et liberté 41  
 LOPPSI 2 12  
 Lyons, Daniel 20

**M**

menaces 50  
   défaillance 46  
   entreprise 43

État 45

piratage 46  
 police 45  
 proches 47

Merzeau, Louise 21, 43

MesInfos 193

messagerie instantanée 125  
   OTR 128

Midata 193

minitel 17

modèle économique 18, 19

mot de passe 168  
   commandements 165  
   stocker 168  
   vulnérabilité 165

moteur de recherche 82

**N**

navigateur 58, 60, 68

  cookie 67  
   mode privé 66  
   protection 61  
   trace 63, 73

navigation 58, 163

  privée 66

New Yorker 11

non répudiation 110

**O**

Ohm, Paul 28

OpenPGP 110, 121

Opéra 60

opt-out 20, 91

ordinateur professionnel 106

OTR 128

**P**

Passpack 168

Patriot Act 187

Petraeus, David 188  
 PGP 110  
 phrase de passe 113  
 PIPA 12  
 pirate box 199  
 pistage 89  
 Piwik 169  
 POP 98  
 porte dérobée 185  
 possibilité d'audit 51  
 Privacy Bill of Rights 192  
 Privacy Enhancing Technologies (PET) 175  
 privacy policies 78  
 Privacyrights 46  
 protocole de courriel 98  
 proxy 135
 

- CGIProxy 172
- extension 141
- HTTP 138
- SOCKS 138
- utilisation 139
- web 138

 pseudonymat 9, 33  
 Psiphon 157  
 publicitaire 91

**R**

Reddit 175  
 RedPhone 163  
 Reporters Sans Frontières 174  
 réseau social 45, 87, 89  
 Riseup 103  
 risque 50  
 risque et menace
 

- différence 51

 risques 178  
 rooter 162

**S**

Safari 60  
 Schmidt, Eric 187  
 Security in-a-box 174  
 signature 114  
 Silent Circle 163  
 site marchand 16  
 Skype 126, 131, 132  
 smartphone
 

- faiblesse 160

 SMS
 

- chiffrer 163

 Soljénistyne, Alexandre 36  
 Solove, Daniel J. 35, 36  
 suicide machine 85  
 surveillance 22  
 surveillance de masse 15  
 système d'exploitation orienté sécurité 168
 

- AnonymOS 169
- Knoppix 169

 Syverson, Paul 183

**T**

Tactical Tech 174  
 Tails 168  
 technologie prédictive 38  
 terms of service 78  
 Terms of Service 79  
 texto
 

- chiffrer 163

 TextSecure 163  
 Tor 151, 171, 183
 

- aider 170
- fonctionnement 152
- Lewman, Andrew 32
- nœud de sortie 172
- pair à pair 155

Vidalia 171  
 trace 8, 76  
   involontaire 77  
   volontaire 77

tracker 21  
 trackers 91  
 tracking 44  
 Turow, Joe 24  
 Twitter 86, 90

## U

Ultrasurf 157  
 user agent 73

## V

Vidalia 171  
 vie privée 8, 40  
   autonomie 4  
   contrôle 5  
   définition 3  
   Montaigne 3  
   quiétude 4  
   secret 4  
 vie publique 7  
 VOIP 131  
 voix sur IP 131  
 VPN 142, 162  
   Anonine 151  
   avantage 151  
   Chine 144  
   choix 147  
   compatibilité 149  
   configuration 145  
   Hidemiyass 187  
   inconvenient 143  
   Ipredator 151  
   moyen de paiement 150  
   Mullvad 151  
   no log 144, 148

OpenVPN 145, 149  
 PPTP 145, 149  
 protocole 149  
 référence 151  
 ressource 146  
 siège social 147  
 vitesse de connexion 150

## W

webmail 98, 101  
   alternatif 103  
   commercial 101  
 whistleblowers 197  
 Wickr 162  
 Windows Live Messenger 126

## X

XMPP 126

## Y

YouTube 83

## Z

Zimmerman, Philip 110